CLAIMS

1. (Previously Presented) A security intrusion mitigation method comprising:

utilizing network spanning tree configuration information to determine an action for mitigating diffusion of intrusive attacks between components associated with a network, wherein said spanning tree information includes an indication of a first internal diffusion risk and a second internal diffusion risk, wherein said first internal diffusion risk is a risk of a first attack diffusing from a first component associated with said network to a second component associated with said network and said second internal diffusion risk is a risk of a second attack diffusing from a third component associated with said network to said second component;

using said internal diffusion risks to determine that there is a higher risk of said first attack diffusing from said first component to said second component than said second attack diffusing from said third component to said second component; and

using said network spanning tree configuration information to perform said action for mitigating diffusion of intrusive attacks automatically at least in part by mitigating said first attack before mitigating said second attack, wherein said action for mitigating includes compensation for functional support of an application associated with said second component that has priority over another application.

2. (Previously Presented) A security intrusion mitigation method of Claim 1 further comprising utilizing said internal diffusion risks to determine components forming a path in said spanning tree configuration with a highest cumulative diffusion impact risk.

3. (Original) A security intrusion mitigation method of Claim 1 wherein said internal diffusion risk includes an asset value factor.

4. (Previously Presented) A security intrusion mitigation method of Claim 3 wherein said asset value corresponds to an economic impact of a disruption to functionality provided by a particular component.

5. (Original) A security intrusion mitigation method of Claim 1 wherein said internal diffusion risk includes an exposure rating factor.

6. (Previously Presented) A security intrusion mitigation method of Claim 5 wherein said exposure rating defines a threshold value corresponding to connectivity of particular component with other components.

7. (Previously Presented) A security intrusion mitigation method of Claim 5 wherein said particular component is assigned an exposure rating value based upon a connectivity distance from a root node.

8. (Previously Presented) A security intrusion mitigation method of Claim 5 wherein said action is implemented in accordance with a highest risk algorithm.

9. (Previously Presented) A security intrusion mitigation method of Claim 5 wherein said network spanning tree configuration information includes information associated with components included in a utility data center and said action is implemented in said utility data center.

10. (Previously Presented) A security intrusion mitigation system comprising:

a means for communicating information;

a means for processing information including instructions for determining a highest risk path that has the highest risk of an attack spreading between network components included in said highest risk path in comparison to risks of attacks spreading between network components associated with other risk paths and automatically mitigating said attack from spreading between said network components included in said highest risk path; and

a means for storing said information, including instructions for storing information describing said highest risk path.

11. (Original) A security intrusion mitigation system of claim 10 wherein said instructions include security management instructions implemented on a network application management platform.

12. (Original) A security intrusion mitigation system of claim 10 further comprising a means for interfacing with a network application management platform.

13. (Original) A security intrusion mitigation system of claim 10 wherein said instructions include attack spread risk determination instructions.

14. (Original) A security intrusion mitigation system of claim 10 further comprising a means for centrally controlling a utility data center operations.

15. (Previously Presented) A computer usable storage medium having computer readable program code embodied therein for causing a computer system to implement security intrusion mitigation instructions comprising:

a component risk determination module for determining that a first risk of a first attack spreading from a first component to a second component is higher than a second risk of a second attack spreading from a third component to a fourth component, wherein said first, second, third and fourth components are included in a network; and

an attack spreading response module for responding to said first risk before responding to said second risk.

16. (Previously Presented) A computer usable storage medium of Claim 15 wherein said first risk is biased based upon an economic value of functions said second component performs.

17. (Previously Presented) A computer usable storage medium of Claim 15 said first risk is biased based upon connectivity of said second component to said first component in said network.

18. (Previously Presented) A computer usable storage medium of Claim 17 wherein said responding includes reducing traffic communication to said second component.

19. (Previously Presented) A computer usable storage medium of Claim 15 wherein said responding includes turning off an interface of said second component to said network.

20. (Previously Presented) A computer readable medium of Claim 19 wherein said responding is performed in accordance with a highest risk analysis.